

三菱電機グループ
情報セキュリティ報告書 2026

目次

■ 目次・編集方針	1
■ ごあいさつ	2
■ 三菱電機グループのビジョン・戦略	3
■ 情報セキュリティマネジメント	
情報セキュリティの基本方針	4
情報セキュリティの体制	5
グローバルガバナンス強化	6
マネジメントの考え方	7
情報セキュリティに関わる規則・ガイドライン	8
情報セキュリティの点検	8
情報セキュリティの教育	9
三菱電機グループの個人情報保護への取り組み	10
三菱電機の個人情報保護への取り組み	10
その他の施策	12
■ サイバーセキュリティに対する取り組み	
サイバー攻撃対策	13
■ 製品セキュリティに対する取り組み	
三菱電機PSIRTの役割	16
三菱電機PSIRTの体制	16
製品セキュリティに関わる法令対応	16
■ OTセキュリティに対する取り組み	
三菱電機FSIRTの役割・体制	17
OTセキュリティ対策の推進	17
■ セキュリティソリューションの提供	
Nozomi活用による	
OTセキュリティソリューション	18
CyberMinderによるCTEMの実現支援	20
SmartCFC/SOC	21
■ 研究開発	
AIの安全な活用を支える情報保護技術	22
■ 第三者評価・認証	
プライバシーマーク取得状況	23
ISMS認証取得状況	23

編集方針

本報告書は三菱電機グループが「活力とゆとりある社会の実現」に貢献するために日々行っている情報セキュリティの取り組みについて、顧客や取引先等をはじめとしたステークホルダーの皆様にご報告することを目的として発行しています。

報告期間

2025年度
(2025年4月1日～2026年3月31日)
2026年4月以降の方針や目標・計画等についても一部記載しています。

報告範囲

三菱電機グループの情報セキュリティの取り組み

報告書の発行時期

2026年10月発行

お問い合わせ先

三菱電機株式会社
デジタルイノベーション事業本部
IT・セキュリティガバナンス部
〒100-8310
東京都千代田区丸の内2-7-3 東京ビル



情報セキュリティ報告書に関する お問い合わせ

※ 本報告書に記載されている会社名、製品名、サービス名などは、各社の商標または登録商標です。

ごあいさつ

変化し続ける脅威を見据え、グローバルな知見と技術を結集して
サイバー空間の安全を守り、持続可能なデジタル社会の実現に貢献します。



三菱電機株式会社
専務執行役
CIO(情報セキュリティ担当)

武田 聡

AI活用やデータサイエンス、DXの進展が著しい一方で、サイバー攻撃の手口は巧妙化し、世界中で脅威が高まっています。AIの発展により、これまで人では気づかなかった脆弱性をAIが高速かつ詳細に把握し、さらにその脆弱性を悪用した攻撃を行うリスクがあります。三菱電機グループは、国内外で幅広い事業を展開しており、サイバーセキュリティを重要な経営課題と認識して取り組んでいます。

AIの活用は、業務の効率化や生産性向上にとどまらず、分析・判断の高度化、新たな価値創出を実現する大きな機会である一方で、その利用に伴うリスクへの適切な対応も不可欠です。特に、AIが扱うデータの適正な管理、利用目的に応じたアクセス制御、機密情報や個人情報の保護に加え、AIを悪用したサイバー攻撃や偽情報の生成、不正アクセスなどへの備えを強化していく必要があります。あわせて、人では発見しきれなかった脆弱性に対して先手を打って備えることが、今後ますます重要になります。

当社グループでは、AIを安全かつ適切に活用するため、ガバナンス体制や運用ルールの整備、データ管理基盤の強化、利用者への教育・啓発など、安心してAIを活用できる基盤づくりを進めています。あわせて、AI技術を活用した脅威検知、監視、分析、インシデント対応の高度化にも取り組み、サイバーセキュリティ対策の向上を図っていきます。

また、グローバルでのセキュリティ体制につきましては、従来は事業部門の情報セキュリティ管理者が海外関係会社を統括していましたが、当社グループでの情報セキュリティ管理のグローバルガバナンス強化及び地域特有の法規制や慣習を鑑みた地域毎の自立的な管理・運営を推進するため、4地域(米州、欧州、アジア、中国)の代表機構にアサインした地域情報セキュリティ統括管理者(R-CISO※1)が海外関係会社を統括することにより、セキュリティ体制を強化しました。

2026年5月に発表しました新中期経営戦略におきましては、中期的に全社で注力する3領域としてスマートエナジー、オートメーション、ディフェンス&スペースを設定しましたが、その中のオートメーション領域に関連する事業として、OTセキュリティを強化事業に設定しました。OTセキュリティにつきましては、昨年度に完全子会社化した米国Nozomi Networks社の技術・製品の当社グループ内での活用も進めています。具体的には、Nozomi Networks社の製品を国内拠点のみならず国内外の関係会社にも順次展開できるよう計画を策定中であり、OTセキュリティの強化を推進しています。

本報告書は、当社グループの情報セキュリティ活動をご紹介しますものです。ご覧いただき、皆様のお役に立つことができれば幸いです。

※1 R-CISO:Regional Chief Information Security Officer

三菱電機グループのビジョン・戦略

近年、サイバー攻撃は高度化・巧妙化し、AIの急速な進化によって攻撃手法もさらに高度化・自動化しており、リスクの対象は、情報システムだけでなく、製品・サービス、工場・設備、クラウドサービス、取引先・委託先を含むサプライチェーン全体へと広がっています。当社グループは、国境を越えたチームワークでサイバー脅威に立ち向かい、健全なサイバー空間を守ることでデジタルイノベーションを促進し、活力とゆとりある社会の実現を目指しています。

この考えの下、グローバルガバナンスを強化し、各地域の法規制や脅威動向に対応した実効性のあるセキュリティ管理を推進しています。また、デジタル基盤「Serendie」とAIを活用した安全なデータ利活用を推進するとともに、Nozomi Networks社の技術・人財と、当社グループが培ってきた制御・運用技術、製造現場の知見を組み合わせ、IT、OT、製品・サービスを横断したセキュリティ強化に取り組んでいます。

これらの取り組みを通じて、グローバルな事業継続と、お客様への安心・安全な価値提供を支えています。

情報管理・セキュリティガバナンス

当社グループ全体が一体となって情報セキュリティ施策を推進するため、体制・役割・責任を明確化し、経営、事業、現場が連携したガバナンスを強化しています。また、グローバルに展開する事業を支えるため、地域ごとの法規制・事業特性を踏まえた管理体制を整備し、海外関係会社を含むグループ全体でのセキュリティレベル向上に取り組んでいます。さらに、平時から重要システムおよび重要データの把握を進め、インシデント発生時においても事業影響を最小限に抑制できる体制の整備に努めています。

ワンストップセキュリティサービス

当社グループは、情報セキュリティ、OTセキュリティ、製品セキュリティ、セキュリティガバナンス、監視・運用、コンサルティングを組み合わせたワンストップセキュリティサービスを構築します。各領域を横断し、リスクの把握、対策の把握、対策立案、導入、監視、対応、改善までを一貫して支援することで、変化する脅威に継続的に対応できる体制づくりに貢献します。

グローバル人材育成

社外のセキュリティエコシステムにおいても活躍できる専門性の高いセキュリティ技術者を育成し、グローバルでの知見共有とセキュリティ水準の向上に取り組んでいます。また、社内CTF※1などの実践的な演習や教育・訓練を通じて、攻撃・防御の両面からセキュリティスキルを高めています。

※1 CTF: Capture the Flag

AI活用によるセキュリティ対応力の強化

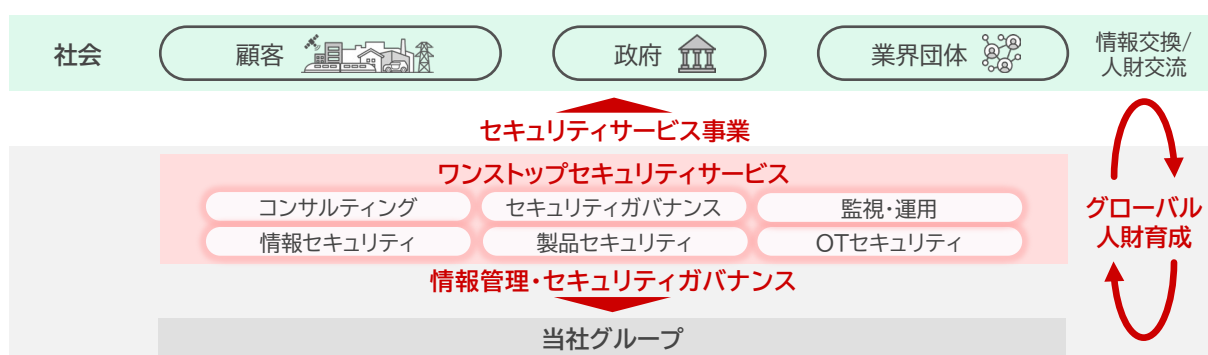
AI利用に関するルール整備、教育、リスク評価を進めるとともに、AI活用によるセキュリティ対応力の強化を重点戦略の一つに位置付けています。AIを悪用した攻撃の高度化・自動化に備え、防御側においてもAIを活用し、環境への影響を早期に把握し、必要な対策を先回りして講じます。また、脅威インテリジェンス機能を持つ体制を強化し、世の中の脅威情報の先読み、影響判定、プロアクティブな対応、自律的な対策実施につなげます。これにより、監視・分析の高度化と運用の効率化を図り、AI時代の高度なサイバー脅威への対応力を高めていきます。

サプライチェーンセキュリティの強化

事業活動のデジタル化と外部サービス利用の拡大に伴い、サプライチェーン全体のセキュリティ確保が重要となっています。取引先・委託先を含む関係先との連携、リスク評価、契約・運用ルールの見直し、インシデント発生時の連絡・対応体制の整備を進めることで、サプライチェーン全体でのリスク低減に取り組んでいます。

エコシステムへの参画と共創

当社グループは、サイバーセキュリティを政府、業界団体、顧客、取引先、パートナー企業、大学・研究機関などの共創によって高めていくべき社会的基盤と捉えています。そして、Serendieを軸としたデータ連携に加え、Nozomi Networks社の技術・人財や社外の多様な組織との連携を通じて、OT、AI、クラウド、ネットワーク、運用サービスを組み合わせた新たなセキュリティ価値の創出を進めています。



情報セキュリティマネジメント

情報セキュリティの基本方針

当社グループでは、急速に高度化・巧妙化が進むサイバー攻撃の脅威に対応するため、サイバーセキュリティと、情報管理・運営体制等のガバナンスの継続的な強化に取り組んでいます。

当社の顧客や取引先等をはじめとしたステークホルダーの皆様からお預かりした情報、営業情報や技術情報、知的財産等の情報資産については、「情報セキュリティ基本方針」の考えに基づき管理しています。

情報セキュリティ基本方針

三菱電機グループは、お客様からお預かりした情報、ならびに当社グループが保有する企業機密・個人情報、情報システムや制御システム等を事業活動の基盤となる重要な情報資産と位置づけています。

当社グループは、技術革新やデジタル化の進展に対応しつつ、これらの情報資産を適切に管理・保護し、安心・安全な製品・サービスを国内外のお客様さまに提供し、社会全体の安全なデジタル環境づくりに貢献します。

この取り組みを実現するため、以下に掲げる方針に基づき、グループ一丸となって情報セキュリティを推進します。

1. 情報セキュリティ体制の構築

当社グループは、経営者層自らが率先し、グローバルな情報セキュリティ管理体制を整備し、情報セキュリティに関連した被害の最小化と迅速な対応を実現します。

2. 法令・規則遵守

当社グループは、法令、契約上の義務等を遵守し、個人情報に関しては、「個人情報保護方針」に基づき、適正に取り扱います。

個人情報保護方針：<https://www.mitsubishielectric.co.jp/privacy/>

3. 情報資産の適切な管理

当社グループは、お客様からお預かりした情報を含めて、事業活動に関連する情報資産を適切に管理します。

4. 情報セキュリティマネジメントの推進

当社グループは、情報セキュリティマネジメントシステムをグローバルに構築し、PDCA(Plan・Do・Check・Act)のサイクルによる主体的かつ継続的な情報セキュリティの維持、向上を図ります。なお、もしもの時にあたっては、OODA(Observe・Orient・Decide・Act)ループを用いて迅速・適正に対応いたします。

5. 安全・安定的な製品・サービスの提供

当社グループは、開発から製造、販売、保守に至る各工程において情報セキュリティ対策を推進し、サプライチェーン全体の信頼性向上を図ることで、安心・安全な製品・サービスの安定的な提供に努めます。

製品セキュリティポリシー：<https://www.mitsubishielectric.co.jp/psirt/policy/index.html>

6. 全従業員に対する教育の実施

当社グループは、個々の従業員の情報セキュリティに関する意識向上こそが管理の基本であるとの認識に基づき、すべての役員、従業員に対して、啓発や教育などの施策を継続的に実施します。

制定日 2005年2月16日

改正日 2026年8月 5 日

情報セキュリティの体制

当社グループの情報セキュリティ体制は、執行役社長を情報セキュリティ管理に関する最高責任者とし、全社情報セキュリティ責任者に任命された情報セキュリティ担当執行役が、情報セキュリティ管理を企画・統括する部門と事業部門の双方を統括する体制としています。これにより、グループ共通の方針・施策と、各事業の実情に応じた運用をより一体的に推進します。

情報セキュリティ統括管理者は、全社情報セキュリティ責任者指示の下、当社グループ全体の情報セキュリティ方針の策定、施策を企画・統括するとともに、顧客のサプライチェーン要求事項や遵守すべき国際標準・慣行等に対して適切な対応を進め、活動内容全般について定期的に報告します。事業部門では、情報セキュリティ責任者の下、情報セキュリティ管理者が傘下の関係会社を含めた自部門に関する情報セキュリティを管理します。

全社情報セキュリティ責任者が定期的に開催する情報セキュリティ管理者会議では、情報セキュリティ管理者に対して当社グループ全体の情報セキュリティ方針の策定や施策の企画等について展開・連携します。

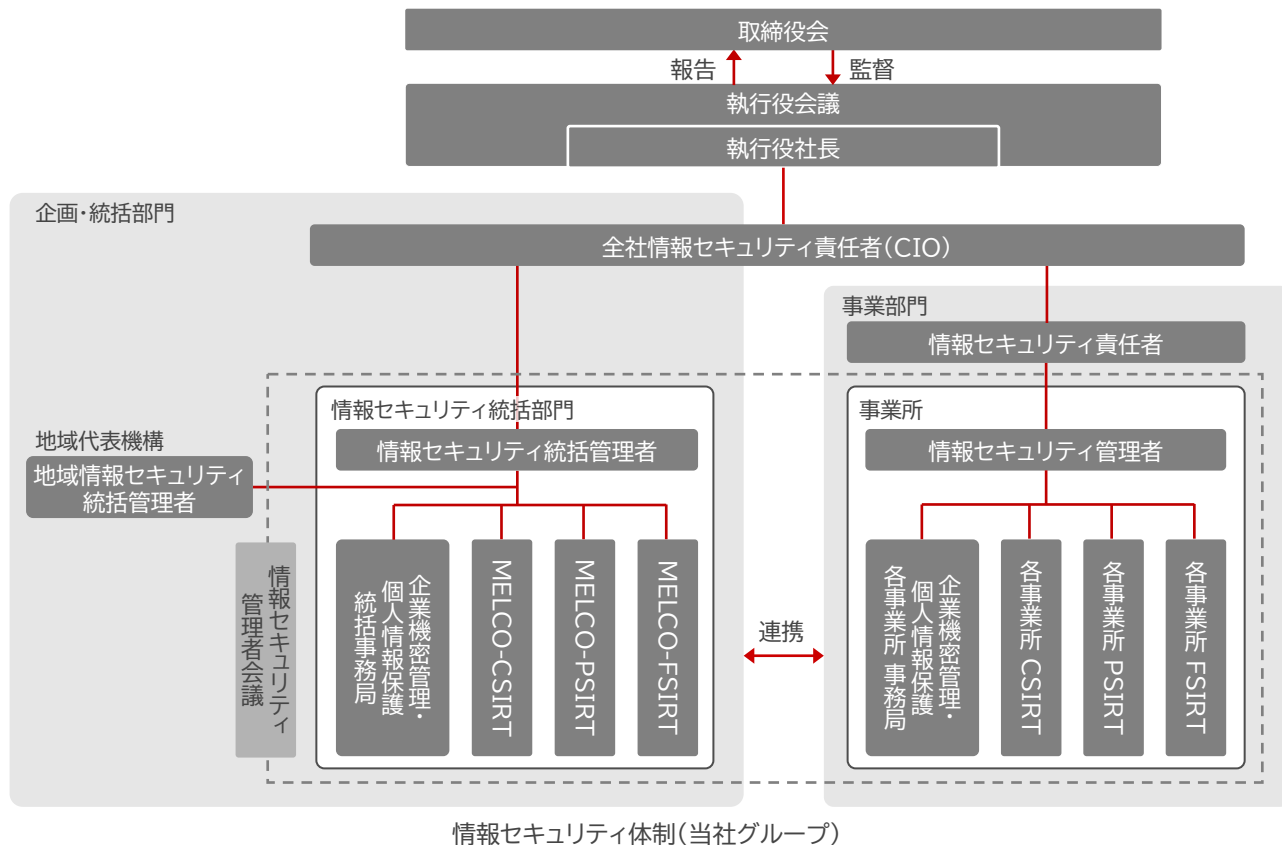
各部門に情報管理、CSIRT※1、PSIRT※2、FSIRT※3の機能を持たせ、情報セキュリティ統括部門が当社グループの情報セキュリティ管理の仕組み、ルール、情報システムのセキュリティ確保、個人情報保護に関する法令遵守や取り組みに関して企画・推進しています。また、インシデント発生時には事業部門と連携し、事業状況を踏まえた総合的な状況判断の下、迅速に意思決定を行い、インシデント対応を進めます。

海外の関係会社については、地域情報セキュリティ統括管理者が、各地域における情報セキュリティ方針の策定および施策の企画・統括・推進を行い、情報セキュリティ管理活動全般をとりまとめます。さらに、情報セキュリティ統括管理者と連携し、当社グループ全体の情報セキュリティ方針の策定および施策の企画を行います。

※1 CSIRT:Computer Security Incident Response Team

※2 PSIRT:Product Security Incident Response Team

※3 FSIRT:Factory Security Incident Response Team



グローバルガバナンス強化

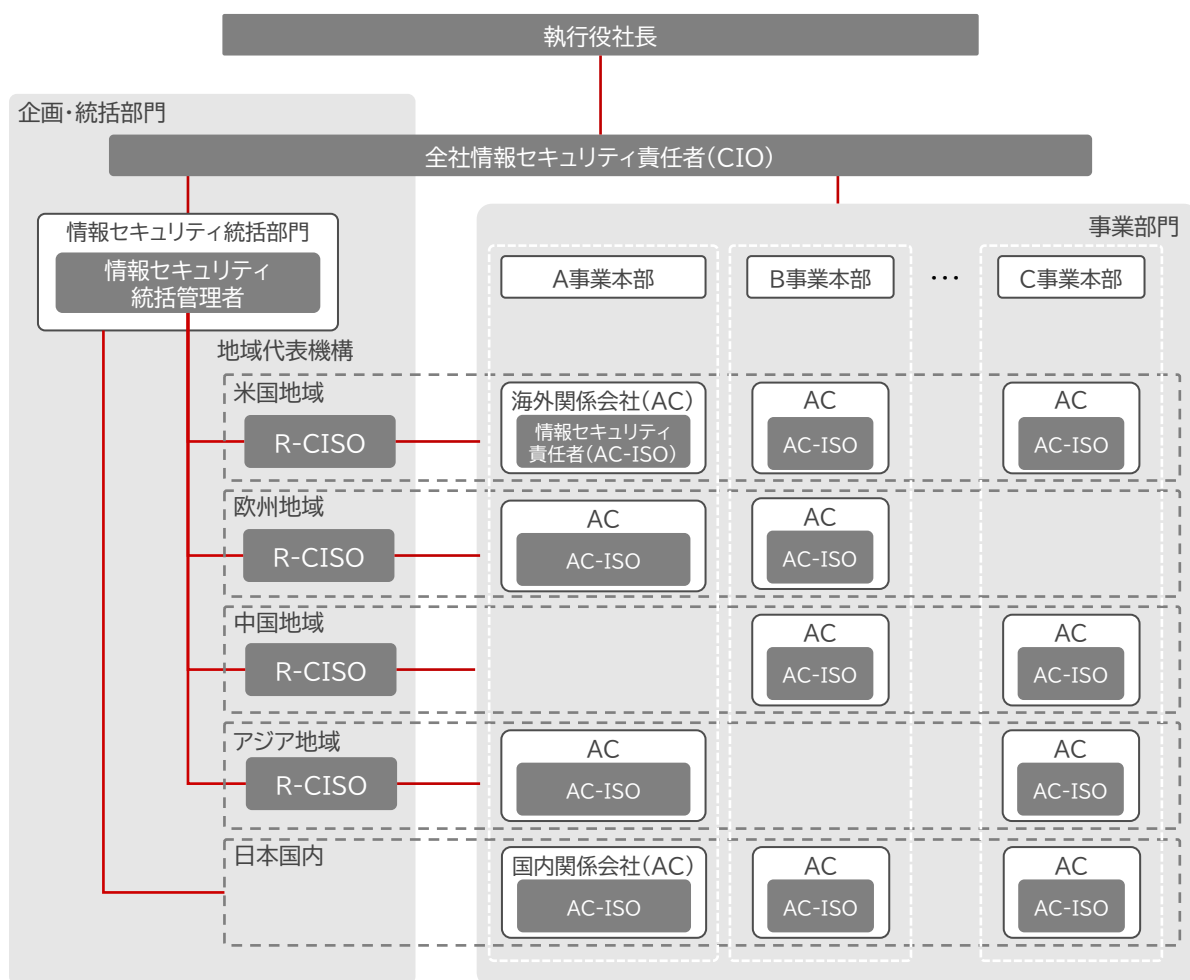
当社グループは、国内外で幅広い事業を展開しており、グローバルにおけるサイバーセキュリティリスクへの対応を重要な経営課題の一つと位置付けています。近年、サイバー攻撃の高度化・巧妙化に加え、欧州のNIS2指令やサイバーレジリエンス法をはじめ、各国・地域における情報セキュリティ関連法令・規制の強化が進んでいます。

これらの環境変化に対応し、海外関係会社を含む当社グループ全体の情報セキュリティレベルを継続的に維持・向上させるため、当社は海外地域ごとの推進体制を強化しています。その一環として、米州、欧州、中国、アジア等の各地域における情報セキュリティ活動を統括・支援する

地域情報セキュリティ統括管理者(R-CISO)を設置し、グローバルでのガバナンス強化に取り組んでいます。

地域情報セキュリティ統括管理者は、全社の情報セキュリティ方針の下、情報セキュリティ統括部門と連携し、各地域・各国の事業環境、法令、商習慣、リスク特性を踏まえた情報セキュリティ活動を推進します。また、海外関係会社の情報セキュリティ責任者(AC-ISO※1)との連携を深め、ガイドラインの展開、法令動向への対応、点検活動、インシデント対応支援などを通じて、地域に根差した実効性の高い管理体制の構築を進めています。

※1 AC-ISO: Affiliated Company – Information Security Officer



海外における情報セキュリティの推進体制

R-CISO : Regional Chief Information Security Officer
AC : Affiliated Company
ISO : Information Security General Manager

マネジメントの考え方

当社グループでは企業機密管理及び個人情報保護の活動をPDCA(Plan・Do・Check・Act)サイクルによる継続的な改善活動として取り組み、企業機密・個人情報を守るために、海外における個人情報の取り扱いなどの外的環境も考慮して、組織的・人的・技術的・物理的からなる4つの安全管理措置を実施しています。

PDCAサイクル

年度初めに年度方針に基づく計画を策定(Plan)し、各種情報セキュリティ施策の展開や従業員への教育を行った(Do)上で、情報セキュリティの運用状況を点検(Check)し、その結果を基に施策などを見直す(Act)ことで、情報セキュリティのレベルがスパイラルアップするよう努めています。

4つの安全管理措置

「組織的」安全管理措置は、管理体制、社内規則、点検/監査など企業機密・個人情報を守るための仕組みであり、業務環境の変化などによりその有効性が失われないよう必要に応じて、見直しています。

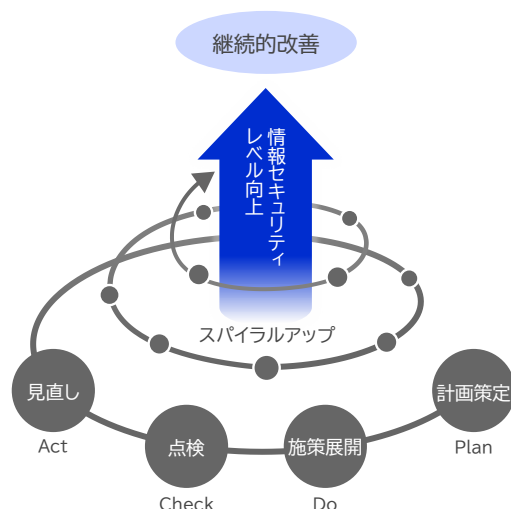
「人的」安全管理措置は、情報セキュリティの施策を従業員に徹底するための教育や労務管理です。

「技術的」安全管理措置は、サイバー攻撃対策などの情報システムセキュリティです。

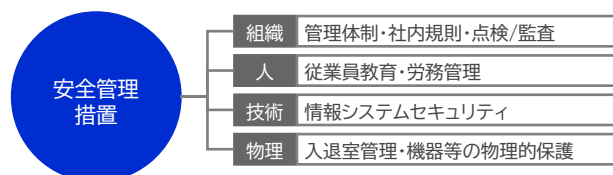
「物理的」安全管理措置は、無関係な第三者が事業所内に入って企業機密や個人情報に触れることを防ぐ入室管理や機器などの物理的保護です。

グローバルでの取り組み

海外関係会社を含めたグループ全体で情報セキュリティレベルを維持・向上すべく、関係会社向けの企業機密管理・個人情報保護に関するガイドラインを制定し、情報セキュリティの体制に則り、各種点検を実施しています。また、日々変化するNIS2指令やサイバーレジリエンス法をはじめとする、グローバルなサイバーセキュリティ関連法令を定期的にモニタリングし、当社グループ一丸となって対応を進めています。



PDCAサイクルによる継続的改善



4つの安全管理措置

情報セキュリティに関わる規則・ガイドライン

情報セキュリティに関わる、個人情報保護方針を実現するために、情報セキュリティに関わる規則・ガイドラインを4つの安全管理措置に沿って整備し、現行の法律に則り、適宜見直しています。

また、個人情報保護についても自国の法令、適用を受ける第三国・地域の法令の遵守はもとより、当社グループにおける共通のガイドラインを関係会社に対しても適用し、個人情報を適切に取り扱い、グローバルレベルで保護します。

項目		基本的な規則
安全管理措置	組織的安全管理措置	企業機密管理規則／個人データ保護ガイドライン
	人的安全管理措置	社員就業規則
	技術的安全管理措置	情報システムセキュリティ管理規則
	物理的安全管理措置	物理セキュリティガイドライン

業務環境の変化に対する対応

基本となる上記規則類に加えて、業務環境の変化に応じて公開ウェブサイトの開示に関する規則、スマートフォンの使用に関する規則、サプライチェーン上の情報セキュリティを

強化するための管理基準などを必要に応じて適宜設けています。

情報セキュリティの点検

当社グループでは、グループ全体の企業機密管理・個人情報保護活動が適切になされているか、またどのようなレベルにあるかを確認するために、PDCAサイクルの中のC (Check)として、本社コーポレート部門、事業本部、事業所及び関係会社にて次の点検活動を実施しています。

これにより、施策などを見直し、PDCAサイクルのA (Act)につなげていきます。

これらの点検活動については、当社を対象とした「企業機密管理規則」及び国内外関係会社を対象とした「情報セキュリティ管理規則ガイドライン」に定めています。

分類	名称	内容など
自己チェック	企業機密管理・個人情報保護に関する自己点検	当社グループ各社でチェックリストを用いて、情報セキュリティの取り組みを自己点検しています。
第三者チェック	企業機密管理・個人情報保護に関する第三者点検	当社事業所間では相互に情報セキュリティの運用状況を確認しています。関係会社の情報セキュリティの運用状況は当社が確認しています。
	個人情報保護の監査(PMS監査)	当社では、執行役社長から指名された個人情報保護監査責任者の指示の下、全社で個人情報の保護状況を確認しています。プライバシーマークを付与された国内関係会社では、各社の監査責任者により同様の確認をしています。

情報セキュリティの教育

当社では、企業機密・個人情報の適切な取り扱いを徹底する企業風土の醸成に努めています。機密等級に応じたファイルのサーバー保管や暗号化など具体的な安全管理措置を従業員が着実に実施できるよう下記の教育プログラムを実施しています。

全従業員への教育

約5万人の全従業員などを対象に情報セキュリティの教育を年1回、eラーニングで実施し、当社の方針、情報漏えい事案の概況、個人情報保護関連法令、不正競争防止法、一人一人が認識すべき安全管理措置（組織的・人的・技術的・物理的）を周知徹底します。また、テレワークの急増やクラウド活用による業務形態・環境の変化に伴い、適宜、従業員向け教育資料を展開しています。2025年度の受講率は100%であり、2026年度も100%を目標といたします。

キャリアパスに沿った教育

新入社員、新任課長、個人情報資産管理者、運営に関わる事務局向けの研修などを通して、各階層や担当業務で求められる役割を果たすために必要な企業機密管理・個人情報保護の教育を実施しています。

不審メール対処予行演習

サイバー攻撃対策として、当社では役員を含む全従業員を対象に「不審メール対処予行演習」を実施し、定期的に不審メールへの対処方法を確認しており、国内関係会社の従業員も同演習に参加できるようにしています。海外関係会社については、地域担当の下、米州、欧州、アジアで地域の実情に合わせて予行演習を実施しています。

その他の個別教育

海外赴任者に対しては赴任前研修の中で、企業機密管理・個人情報保護に関する海外でのリスク、海外での情報漏えい事案の事例について教育しています。

三菱電機グループの個人情報保護への取り組み

基本姿勢

当社グループは、企業理念を「私たち三菱電機グループは、たゆまぬ技術革新と限りない創造力により、活力とゆとりある社会の実現に貢献します」と定め、様々な事業を展開しています。私たちは、お客様、株主・投資家、取引先、従業員など、様々なステークホルダーから貴重な情報をお預かりしています。その中でも、個人情報等は特に重要な財産のひとつであり、私たちは個人情報を適切に取り扱うことを社会的責務と考えています。

当社グループは、各国・地域の法律に基づいた8つの原則に従って個人情報を取り扱い、体制の確立と適切な取り組みによって改善・維持に努めています。

個人情報の取り扱いに関する原則

当社グループでは、お客様からお預かりした大切な個人情報情報を以下の原則に従って取り扱います。

- (1)適法性の原則：関係法令に従い、適切に個人情報を取得し、取り扱います。
- (2)公平性及び透明性の原則：個人情報の取り扱いについて、お客様の観点に立って適切なタイミングで、容易な手段を用いて分かり易くお知らせします。

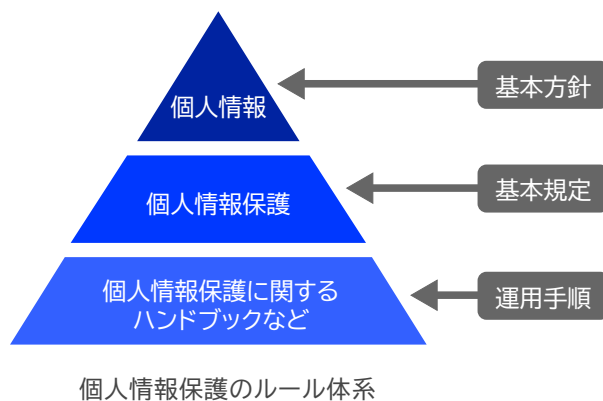
- (3)取り扱い目的の制限の原則：明確かつ適法な目的の下で個人情報を取得し、その目的の範囲内において取り扱います。
- (4)データの最小化の原則：取り扱い目的の範囲において必要なものに限定して個人情報を取り扱います。
- (5)正確性の原則：可能な限り個人情報を正確に保ちます。必要な場合にはデータを更新します。
- (6)保存制限の原則：取り扱い目的に応じて定めた必要な保存期間の中で個人情報を取り扱い、保存期間が終了した際には、適切な方法で削除します。
- (7)完全性及び機密性の原則：不正アクセスや紛失、破壊、改ざん、漏えいなどから保護するために、個人情報に対して必要なセキュリティ対策を講じます。
- (8)企画段階でのプライバシー保護の原則：個人情報を取り扱う企画の段階から、上記の原則を遵守するために保護措置を講じます。

三菱電機の個人情報保護への取り組み

個人情報保護マネジメントシステムの構築

当社では、「個人情報保護方針」及び「個人情報の保護に関する規則」を制定し、日本工業規格「JIS Q 15001:個人情報保護マネジメントシステム—要求事項」に準拠した体制を構築・整備の上、当社従業員等に個人情報保護を周知徹底し、個人情報保護活動に取り組んでいます。

2008年1月には個人情報について適切な保護措置を講ずる体制を整備している事業者として認定を受け、プライバシーマークを取得しました。2026年1月には、9回目の更新手続きを完了しています。



各種アンケートやお買い上げいただいた製品の登録、アフターサービスなどを通じて入手したお客様の個人情報は、「個人情報保護方針」の考えに基づき管理しています。

さらに、当社ではプライバシーマークを取得しており、個人情報の適正な取り扱いに努めています。

個人情報保護方針

三菱電機(以下、「当社」といいます。)は、技術、サービス、創造力の向上を図り、活力とゆとりのある社会の実現に貢献していきます。このような活動を通じて、当社はお客様や関係の皆様から、様々な情報をお預かりしており、個人情報については個人の重要な財産であることから、法律に則って適切に保護し、正確かつ安全に取扱うことは企業の社会的責務と考えます。当社は、経営の一環として個人情報保護マネジメントシステムを確立し、当社従業員(役員・社員・パートタイマー・アルバイト・派遣社員などを含む)及びその他関係者に個人情報保護を周知徹底させて以下の取り組みを実行するとともに、改善・維持に努めてまいります。

1. 個人情報保護の目的

個人情報を適正かつ効果的に活用し、個人情報の有用性に配慮しつつ、個人の権利利益を保護することを目的とします。

2. 個人情報の利用目的

ご本人様に明示した利用目的の範囲内で、事業遂行上必要な場合のみ個人情報を利用します。また、目的外の利用を行わないために必要な措置を講じています。

3. 個人情報の取得

適法かつ公正な手段によって個人情報を取得します。直接、ご本人様より取得する場合は、利用目的等の必要事項を明示し、同意を頂きます。

4. 個人情報の開示・提供

委託業務や協業等に際して第三者に個人情報を開示・提供する場合には、ご本人様の同意を取得します。

5. 個人情報の取り扱い

(1) 個人情報保護に関する法令等の遵守

当社は、個人情報保護に関する法令、国が定める指針及びその他規範を遵守します。

(2) 個人情報の漏えい・滅失又は毀損の防止(安全管理措置等)及び是正に関すること

個人情報への不正アクセス、紛失、破壊、改ざん及び漏えい等を未然に防止するため、合理的な安全対策とともに、必要な安全管理措置を講じます。また、毎年、個人情報の取り扱い状況について、全部門を対象に監査を実施し、是正処置を実施しています。この監査では、最新の漏えいリスクや課題を全部門で再確認し、同様の事象が発生しないよう改善に努めています。

(3) 個人情報保護マネジメントシステムの構築・運用

当社は、「JIS Q 15001:個人情報保護マネジメントシステム—要求事項」を基に個人情報保護マネジメントシステムを構築し、運用しています。一般財団法人 日本情報経済社会推進協会の審査を受審し、個人情報の適切な取り扱いを行う事業者に与えられる「プライバシーマーク」の付与認定を受けています。今後も、個人情報マネジメントシステムを継続的に改善しながら、個人情報を保護します。



6. 個人関連情報の取り扱い

当社のウェブサイト等にて、位置情報・IPアドレス・クッキー情報等の個人関連情報を取り扱う場合は、ご本人様に利用目的を通知し、同意を取得することがあります。

7. ご本人様からのお問い合わせへの対応

ご本人様から個人情報の開示、訂正、削除、利用停止等を求められたとき、及び苦情、相談等のお問合せを受けたときは、遅滞なく対応いたします。また、個人情報を正確かつ最新の状態に保つよう努めます。

制定日 2004年4月16日

改正日 2022年4月 1 日

三菱電機株式会社
執行役社長 漆間 啓

個人情報の適切な取り扱い

個人情報は利用目的を特定するなど適切に取得し、利用するときは「利用目的の範囲を超えて利用しない」、「第三者に提供するときはあらかじめ本人の同意を得る」など、個人情報を適切に取り扱っています。また、サイバー攻撃による流出リスクにも備えるべく、サーバー保管や暗号化対策などの安全管理措置を一層強化していきます。

プライバシーマーク

当社及び「第三者評価・認証」に記載の国内関係会社では、プライバシーマークを取得しています。

マイナンバーへの対応

マイナンバー制度に対応した社内規定に則り、厳格な管理と適切な取り扱いに努めています。マイナンバーを取り扱う従業員に対して、個別に教育しています。

EU一般データ保護規則(GDPR)、 中国個人情報保護法への対応

EU一般データ保護規則(GDPR※1:2018年5月施行)や中国個人情報保護法(2021年11月1日施行)等、当社において各国・地域法が定義する個人情報を移転、取り扱う場合には当該国・地域法令の要求に従い、適切に保護します。

※1 GDPR:General Data Protection Regulation

その他の施策

取引先・委託先管理

企業機密・個人情報を他社に委託する際は、適切に秘密保持契約を締結した上で、セキュリティ・個人情報保護上の理由から取引・委託先に求める事項を契約書に記載しています。

委託先に渡した企業機密・個人情報が適切な管理の下で取り扱われていることを確認するために、委託先が適切な保護水準を維持しているか評価・選定し、契約後も定期的に利用及び管理状況の報告を受けるなど、適切に監督しています。

サプライチェーン強化に向けたセキュリティ対策評価制度への対応も併せて進めてまいります。

AIでの予兆検知による漏えい対策

経済安全保障の観点及び企業競争力維持の観点から、重要な情報の保護への重要性が高まる中、「人を介した情報漏えい」への対策強化が一層必要とされています。

従業員の職務環境の安心・安全を確保し、当社技術情報・資産の保全を強化するため、AIを活用したメール確認など予兆検知型の漏えい対策を導入しています。

AI活用によるセキュリティリスクの管理

AIの活用を積極的に推進する一方で、情報漏えいや不適切な利用などのセキュリティリスクにも十分に配慮し、適切な管理体制の下で運用を進めています。

サイバーセキュリティに対する取り組み

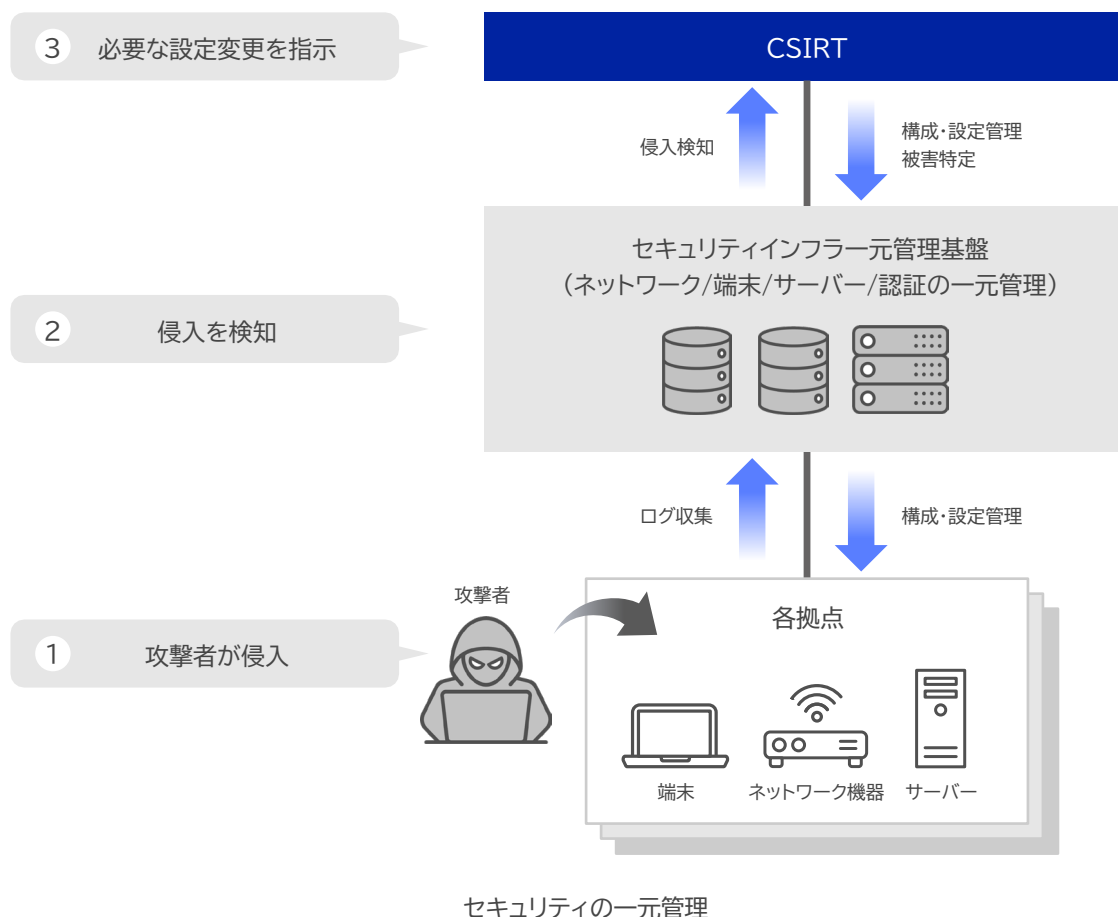
当社グループでは、情報セキュリティに対する取り組みとして、ITインフラのサイバー攻撃対策や物理的なセキュリティ対策を行っています。

サイバー攻撃対策

企業に対するサイバー攻撃は、年々巧妙かつ多様化しており、大きな脅威となっています。

その対策として、当社グループではネットワークや端末、サーバー(クラウド)の一元管理と、「多層防御」の導入に取り組んでいます。「多層防御」によりサイバー攻撃の防御、不審な兆候及び侵入の検知を可能とし、さらに、即時対応する体制を整えることで、被害を防止するとともに、最小化しています。

また、オフィスのほか、テレワークや出張先からのアクセスによる業務に対応するため多要素認証を導入し、認証を一元的に管理しています。さらに、常に外部から多くの脅威にさらされているインターネット公開ウェブサイトについては、セキュリティレベルを保つために当社が認定したウェブサイトのみを公開するように取り組んでいます。



多層防御

当社グループでは、「多層防御」として「ネットワーク」、「端末」、「サーバー(クラウド)」の3階層の技術的なセキュリティ対策を実施しています。

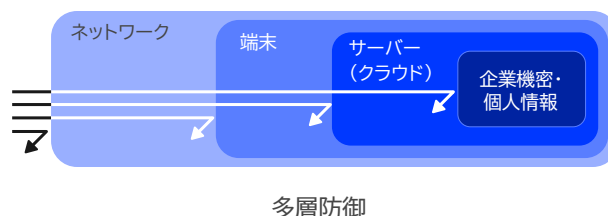
ネットワークでのセキュリティ対策では、インターネットと社内ネットワークの接続点に様々なセキュリティ対策機器を配置し、メールやウェブなどの通信を制御・監視します。それにより、社内への不正アクセスやマルウェアの侵入を遮断し、外部への情報漏えいを防止しています。さらに社内ネットワークでは端末とサーバー間、異なる製作所間での通信を厳密に制御・管理することで、被害の局所化に努めており、今後もこれらの対策を強化していきます。

端末のセキュリティ対策では、端末へのマルウェア感染を防ぐために、端末を一元的に管理し、マルウェア対策ソフトによるマルウェア検知・駆除や、ソフトウェアの脆弱性を修正するセキュリティパッチの適用を徹底しています。また、不審なふるまいを検知する機能(EDR※1)を全端末に配備し、対策を強化しています。さらに、情報システムにアクセスする際には2つ以上の要素の認証を組み合わせる多要素認証(端末認証)を導入し、セキュリティ対策を強固にしています。

クラウドの活用が進むサーバーに対しては、脆弱性の定期的な診断の他、通信やクラウドの運用を監視します。それにより、重要な情報が格納されるサーバー(クラウド)において堅牢な環境を維持できるようにしていきます。

サーバーやクラウドに格納される企業機密・個人情報に対しては、「最小権限の原則」に基づいたアクセス制御と

暗号化を適用します。これらの情報管理については、規則の整備と徹底、従業員教育、点検活動もあわせて実施しています。

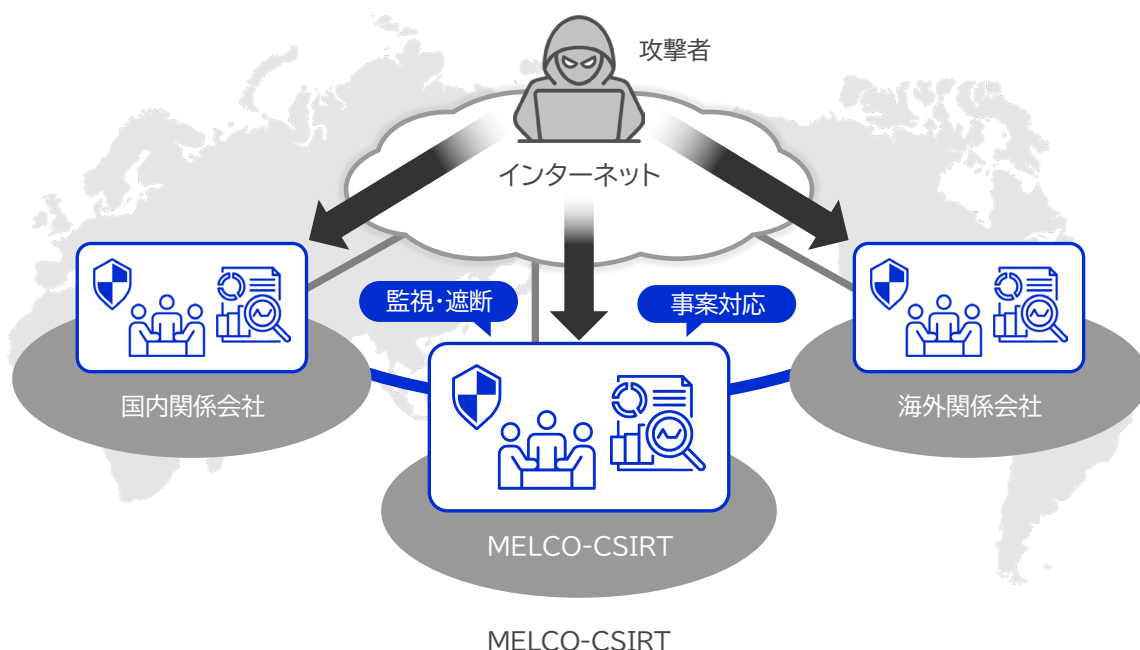


緊急対応体制

当社グループでは、サイバー攻撃に対する監視と事案発生時の即時対応のため、MELCO-CSIRT (Mitsubishi Electric Corporation Computer Security Incident Response Team)を設置しています。

従来は対応が不十分であった国内外の関係会社に対する監視体制も整えました。前述の通信監視により不審な挙動を検知することでサイバー攻撃をいち早く見つけ、遮断します。また、端末側ではマルウェアの検知情報や端末のセキュリティ対策状況などを収集、把握することができます。万一、事案が発生した場合は、上記の仕組みを駆使することで即座に被害状況を把握し、迅速で適切な対処・復旧を行い、被害を可能な限り抑えます。その後、事案を詳細に分析し、事案発生部門による恒久対策の実施を支援します。

※1 EDR:Endpoint Detection and Response



テレワーク時のセキュリティ対策

出張時のモバイル勤務以外にも在宅勤務やサテライトオフィスの利用など、多様化するワークスタイルに対応してテレワークの活用が進んでいます。

一方で、ネットワークやクラウドの活用によって業務環境も多様化し、従来の社内システムとインターネットとの境界を防御するセキュリティ対策では十分に対応できない状況も起こり得ます。そのため、VPN(仮想専用通信網)接続により通信を暗号化し、安全性を確保するとともに、多要素認証も導入し、より強固なセキュリティ対策を行っています。

我々は、在宅勤務、サテライトオフィス勤務、モバイル勤務(出張)のいずれに対しても、サイバー攻撃から防御するためのセキュリティ対策に引き続き取り組んでいます。

インターネット公開ウェブサイト管理

当社グループでは、過去に発生した不正アクセスによる事案を契機に、セキュリティレベルを保つために当社が認定したウェブサイトのみ公開するように取り組んでいます。

事前にセキュリティ検査を実施して不具合を解消したウェブサイトでなければ、公開を許可していません。また、インターネット上の公開ウェブサイトを定期的に点検して、管理状況を把握することで、不要なウェブサイトを廃止する他、セキュリティ対策が不十分なウェブサイトについてはセキュリティ対策を強化しています。

製品セキュリティに対する取り組み

三菱電機PSIRTの役割

当社では、製品・サービスのセキュリティ品質に対応する社内の体制として三菱電機PSIRT(Product Security Incident Response Team)を構築し、製品・サービスの情報セキュリティに対し全社で取り組んでいます。

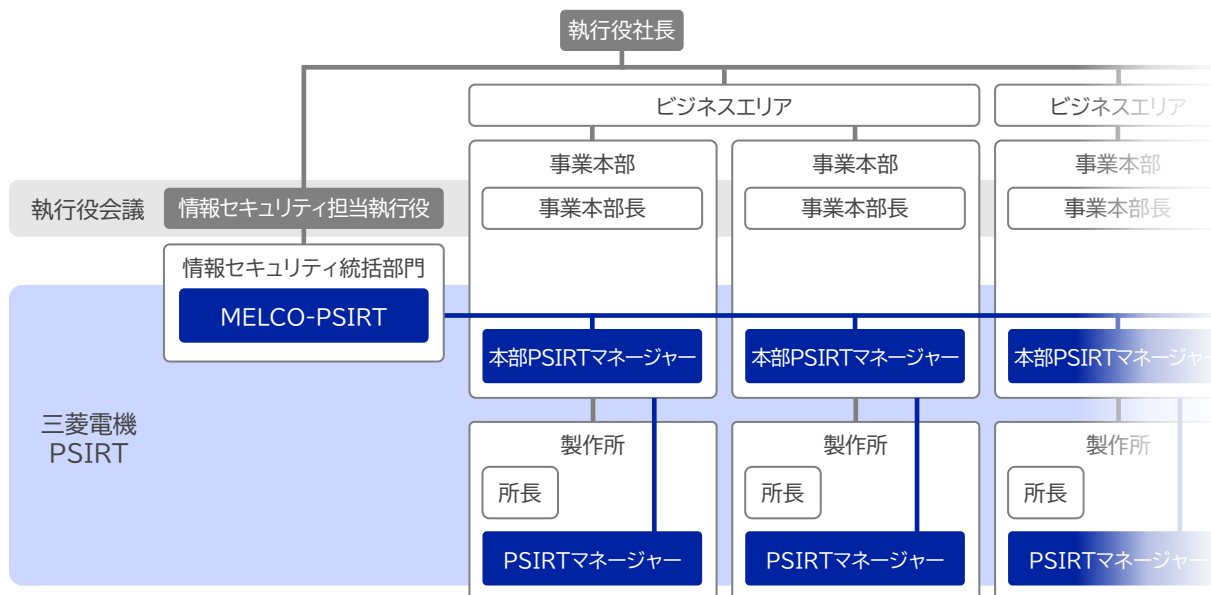
三菱電機PSIRTは、右記を実施することを役割としています。

- お客様へ提供している製品・サービスの脆弱性に関する情報収集
- 製品の設計・製造部門及びサービスの運用部門と連携し発見された脆弱性への迅速な対応
- 製品やサービスを提供する前の段階で脆弱性を作り込まないようにするための設計・開発手法の導入を推進
- 製品・サービスの開発に関係する全ての役員及び従業員に対する必要なセキュリティに関する教育
- 脆弱性に関する情報・対策のお客様への公開

三菱電機PSIRTの体制

当社では、本社に対外的な窓口となるMELCO-PSIRT(Mitsubishi Electric Corporation Product Security Incident Response Team)を設置し、各事業本部に

本部PSIRTマネージャーを配置し、さらに全ての製作所にPSIRTマネージャーを配置して、全社で製品・サービスのセキュリティ品質に対して取り組んでいます。



三菱電機PSIRTの体制図

製品セキュリティに関わる法令対応

近年、デジタル化の進展に伴い、サイバー攻撃による社会への影響が増大していることから、EUのCyber Resilience Actを始め、各国で製品のセキュリティ対応

を求める法規制が強化されています。当社では、製品・サービスのセキュリティ品質への対応に加えて、各国の法令要件を遵守すべく、事業横断で対応に取り組んでいます。

OTセキュリティに対する取り組み

三菱電機FSIRTの役割・体制

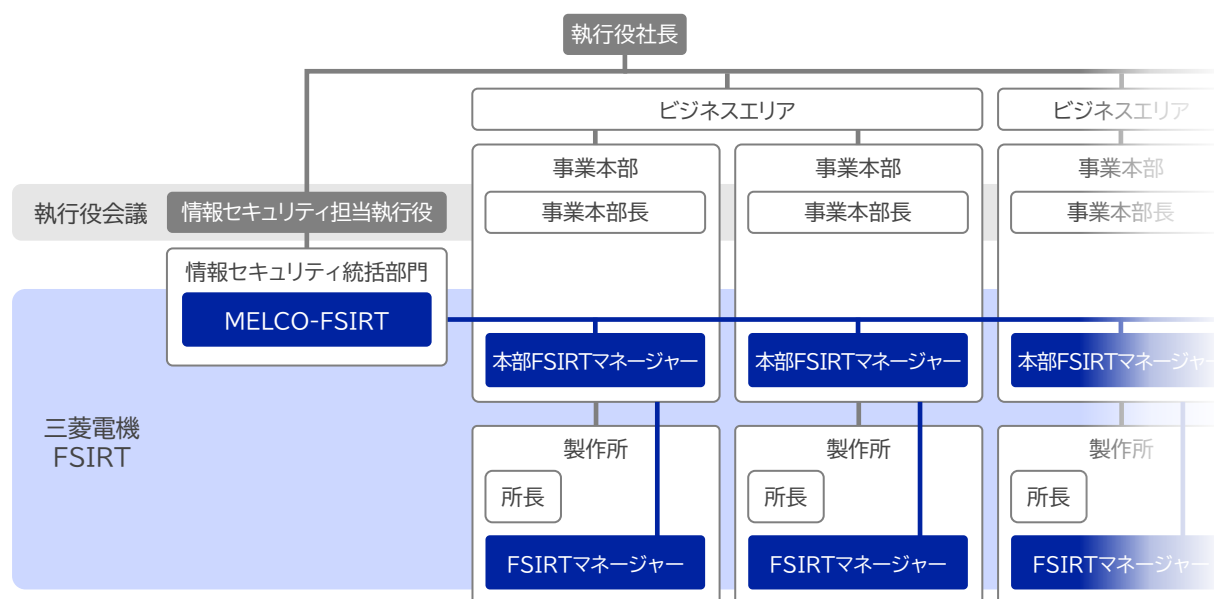
インターネットなど外部との接点を持たずクローズした環境で稼働していた工場の現場にも、IoTやDX、テレワークといった様々な新技術、環境変化の流れが押し寄せてきており、工場もオープンな環境で稼働するようになってきました。

その結果、今まで無縁だったサイバー攻撃の脅威が工場にまで及び、工場停止など重大な被害が近年多発しています。

当社では、三菱電機FSIRT（Factory Security Incident Response Team）を構築し、当社グループの工場に対するサイバーセキュリティ対策の強化に全社で取り組んでいます。三菱電機FSIRTは、情報セキュリティ統括部門内に組織するMELCO-FSIRT（Mitsubishi Electric Corporation Factory Security Incident Response Team）、各事業本部に配置する本部FSIRTマネージャー、各製作所に配置するFSIRTマネージャーにより構成されます。

各組織の役割としては、MELCO-FSIRTが全体統括を担い、全社で発生した問題解決を支援します。また、その対応をとおして得た知見やノウハウを蓄積し、全社の取り組みを改善します。FSIRTマネージャーはMELCO-FSIRTと連携し、製作所内の関係部門をとりまとめます。平時では自組織の状況に合わせ、対策の検討と推進を担い、有事ではインシデント対応を主導します。本部FSIRTマネージャーもMELCO-FSIRTと連携し、インシデントが発生した製作所の後方支援を行います。また事業本部が管轄する関係会社のOTセキュリティに関わる業務をとりまとめます。

各組織は、平時・有事で組織間連携ができる体制としており、OTセキュリティ対策を当社として適切かつ円滑に推進できるよう活動しています。



三菱電機FSIRTの体制図

OTセキュリティ対策の推進

当社グループではOTセキュリティ対策として、製作所における監視の適用を進めており、2026年1月に当社グループの一員となったNozomi Networks社の製品（以下、「Nozomi」という）の導入を推進しています。

導入や運用で出てきた様々な課題は現場の部門と連携しながら解決し、得られたノウハウなどは、お客様向けのOTセキュリティソリューションにも活用できるよう取り組んでいます。

セキュリティソリューションの提供

Nozomi活用によるOTセキュリティソリューション

製造現場や社会インフラでは、IoT、クラウド、リモート保守、IT/OT連携の進展により、OT環境が外部ネットワークとつながる機会が増えています。これに伴い、サイバー攻撃による生産停止、設備停止、品質影響、事業継続リスクへの対応が重要な経営課題となっています。一方で、OT環境では、24時間365日の安定稼働、古いOSや未更新機器の継続利用、産業用プロトコルへの対応など、ITとは異なる前提条件があり、一般的なITセキュリティ対策をそのまま適用することは困難です。

OTセキュリティの主な課題

OTセキュリティには、主に以下の課題があります。

- ・ OT環境の実態が見えない：接続機器、通信経路、利用プロトコル、構成変更を把握しづらい
- ・ リスクの優先順位が分からない：脆弱性、異常通信、影響範囲を踏まえた対策判断が難しい
- ・ OT特有の環境に対応しづらい：安定稼働を優先するため、停止を伴う更新や対策が実施しづらい
- ・ 継続的な監視・運用が難しい：多拠点管理、異常検知、SOC^{※1}連携、運用改善を継続する体制が必要

※1 SOC:Security Operation Center

Nozomiによる解決

Nozomiは、OTネットワーク上の通信をもとに、接続機器、通信経路、利用プロトコル、脆弱性、異常通信を可視化します。構成図や台帳だけでは把握しきれない現場の実態を、実通信ベースで把握できるため、OT環境のリスク分析や対策優先度の判断に活用できます。また、ネットワーク可視化技術、侵入検知ソリューション、脅威検知ソリューション、AIリスク分析、AIセキュリティ分析、AI運用支援により、OT環境における異常の早期検知と継続的な監視・運用を支援します。

三菱電機ソリューションの特長

当社は、OT領域で培ってきたアセスメントノウハウ、セキュリティコンポーネントを組み合わせた提案力、OT知見とITセキュリティで培ったSOC運用力を活かし、Nozomiの可視化・検知・AI分析技術を最大限に活用します。リスクアセスメント、対策立案、導入、監視、運用改善までを一貫して支援することで、お客様の現場に適したOTセキュリティ対策を実現します。

当社は、Nozomiを活用したOTセキュリティ対策を自社工場でも実践しており、そこで得た知見をお客様向けソリューションにも活用しています。



OT環境の可視化から運用改善まで、ワンストップで支援

三菱電機グループでの適用事例紹介

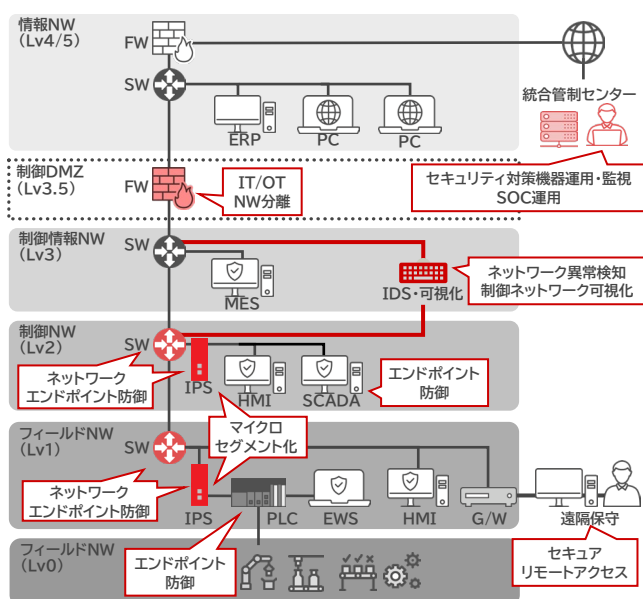
当社のOTセキュリティソリューションは、当社グループの自社工場でも実践しています。本ページでは、その適用事例を通じて、実際の課題と対応方法、社外提供につながるノウハウを紹介します。

社内適用時に直面した課題

実際の工場では、主に以下の課題がありました。

- 管理されていない機器と異常通信の検出
USBや持ち込み端末、脆弱性のある機器など、ファイアウォールを経由しない侵入経路への対応
- セグメント化と侵入防御
脅威の侵入後も、他の生産ラインや設備へ被害が拡大しないよう、OTネットワーク内の防御
- セキュリティポリシーの一元管理
外部ベンダによるリモートアクセスなど、複数の接続経路を安全に管理し、不正アクセスのリスクを低減するための仕組み

以上3つの課題は、いずれもゼロトラスト※1の考えに基づいています。多様な機器が混在するOTの現場では、「ネットワークは閉じたものである」という前提に頼ることなく、社内外を問わず、接続元や端末の状況を確認した上でアクセスを制御する「ゼロトラスト」の考え方が重要となっています。



OTのネットワーク各層で防御

OT知見を活用した生産現場の構築

課題に対し、複数の対策を組み合わせ対応しました。

- (1) Nozomiのソリューションにより、OTネットワーク上の接続機器、通信情報、OS・ファームウェア、使用プロトコルを可視化しました。これにより、管理されていない機器や脆弱性のある機器、異常通信を把握し、リスク分析と対策優先度の判断につなげました。
- (2) TXOne Networks社のEdgeIPSにより、OTネットワーク内を生産プロセスや機能ごとに分割し、攻撃と思われる通信が他のセグメントへ広がらないよう防御しました。
- (3) Dispel社が提供するセキュアリモートアクセスソリューションを活用し、外部ベンダなどのリモートアクセス経路を一本化することで、不正アクセスリスクの低減を図っています。

これらの対策に加え、現場のセキュリティを常時監視する組織を立ち上げ、不正アクセスに対する迅速な分析や対応を24時間365日体制で実施しています。監視によって得られた情報をもとに課題を抽出し、新たな対策立案から導入へつなげるサイクルを回すことで、継続的なセキュリティ強化を実現しています。

三菱電機だから実現できたポイント

当社は、生産現場を理解した上で、設備、ネットワーク、運用、保守の実態に応じた課題抽出と対策設計を行いました。セキュリティ強化だけでなく、生産を止めないことを前提に、可視化、侵入防御、リモートアクセス管理、監視運用を組み合わせた多層的な対策を構築しています。

自社適用で培ったノウハウを、お客様向けソリューションへ展開

当社は、自社工場でのOTセキュリティ適用を通じて、現場課題の抽出、対策設計、導入、監視、運用改善の知見を蓄積しています。この実践知を活かし、お客様の生産現場においても、セキュアな環境と安定した生産稼働を両立するOTセキュリティソリューションをワンストップで提供します。

※1 ゼロトラスト:社内外問わず、全て不正アクセスの可能性があるという前提でチェックするという考え方

CyberMinderによるCTEMの実現支援

三菱電機デジタルイノベーション株式会社

セキュリティ運用を支えるCyberMinder

CyberMinderは、当社が提供するマネージドセキュリティサービス群です。NIST※1のサイバーセキュリティフレームワークに沿って、セキュリティ診断、脆弱性管理、監視・運用、インシデント対応等をワンストップで支援します。



継続的な脅威露出管理「CTEM」

近年、クラウドサービスやSaaSの普及、リモートワークの定着により企業のIT資産は拡大・分散し、従来の組織管理だけでは把握しきれない設定不備や攻撃対象領域の増大が課題になっています。さらにサイバー攻撃は高度化・巧妙化しており、継続的な管理が重要です。こうした背景から、攻撃者視点で資産を継続的に把握し、リスクを優先順位づけして運用する「CTEM(Continuous Threat Exposure Management)」が注目されています。

CTEMは、組織が直面するリスクを客観的に評価・改善していくためのフレームワークで、5つのステップで構成されています。

CyberMinderによるCTEMの実現支援

CTEMの5つのステップに対し、CyberMinderの3つのサービスを活用することで、IT資産の把握および継続的な脆弱性管理を実現できます。

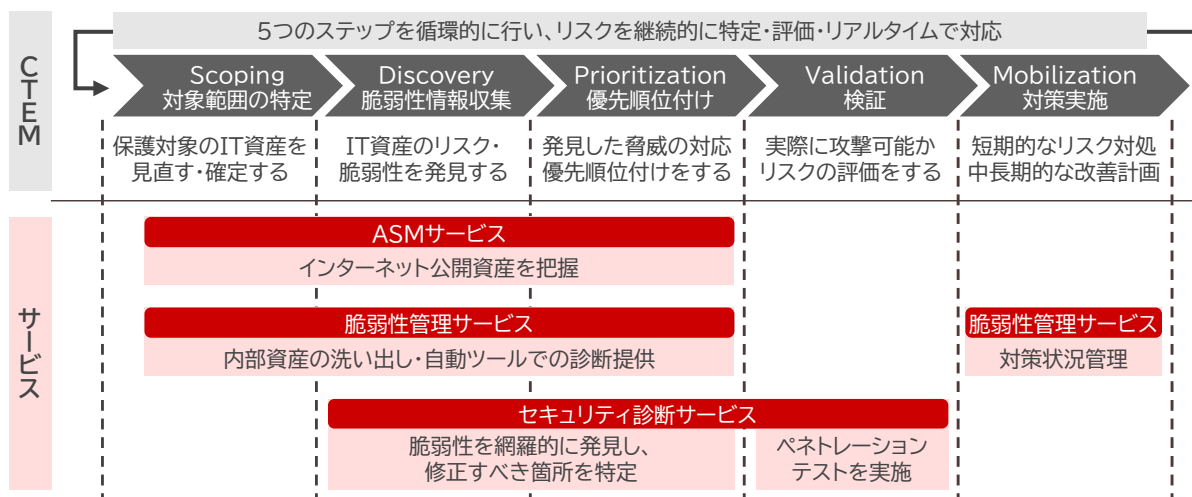
- ASM(Attack Surface Management)サービス
攻撃者の視点でインターネット公開資産を把握し、発見したIT資産の脆弱性を簡易チェックします。
- 脆弱性管理サービス
自動ツールにて広く、漏れなく脆弱性を把握し、継続的に脆弱性を管理します。
- セキュリティ診断サービス
アナリストがピンポイントに深く正確に診断を行い、その対応策までレポートで報告します。

お客様の安全なIT環境への貢献

CyberMinderのサービス群を組み合わせることにより、CTEMの各ステップを継続的かつ網羅的に支援し、お客様のIT環境の安全性向上につなげることができます。

三菱電機グループは、24時間365日の監視・運用やインシデント対応のノウハウと、IT・OT双方の知見を活かし、お客様の事業継続とサイバーレジリエンスの向上に貢献していきます。

※1 NIST:National Institute of Standards and Technology, 米国国立標準技術研究所



CTEMのステップと当社の提供サービス

Smart CFC/SOC ～次世代セキュリティ運用の標準化基盤～

三菱電機デジタルイノベーション株式会社

当社は、MSSP※1としてSOCを運営し、セキュリティ監視・運用サービスを提供しています。近年、AIの悪用によりサイバー攻撃は高度化・巧妙化し、攻撃件数も増加しています。これに伴い、お客様からは、増加するアラートや多様なセキュリティ機器のログを横断的に把握し、脅威を検知した際に速やかに通知・対応することが求められています。

そのため、従来の人手を介した対応に代わり、AIの活用と自動化を軸に、監視対象の拡大にも柔軟に対応できる次世代監視基盤が必要となっています。こうした高度かつ迅速な監視を実現するため、CyberMinderの監視基盤である、Smart CFC/SOC※2基盤を開発しました。

Smart CFC/SOC基盤の特長

- ① 多様なセキュリティ機器ログを一元的に活用
ログ収集インターフェースの標準化により、様々な機器のログに対応し、効率的なログ管理を実現します。
- ② 迅速で安定した一次対応を実現
アラート調査、分析、通知の仕組みを自動化し、迅速かつ安定したセキュリティ運用を提供します。
- ③ リーズナブルにログ分析機能を利用

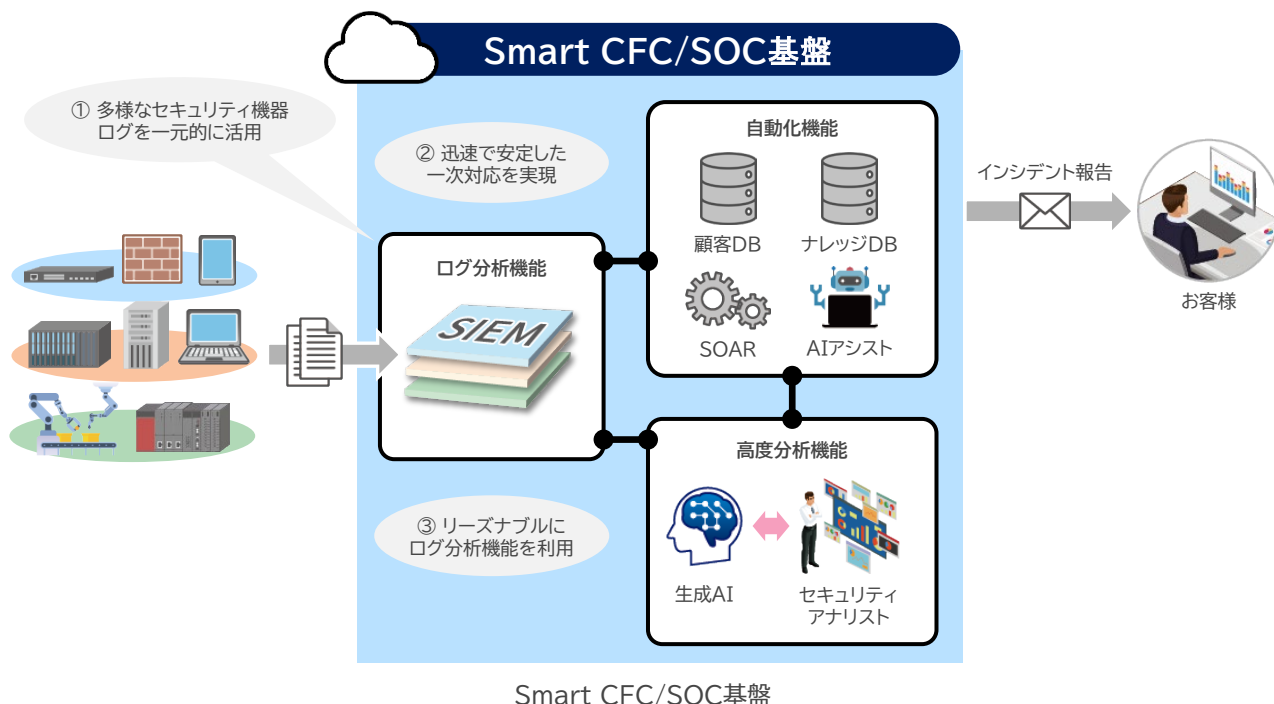
- ③ リーズナブルにログ分析機能を利用
ログ分析基盤をマルチテナントで提供することで、高コストになりがちなログ分析機能をリーズナブルにご利用いただけます。

今後の展望

今後は、生成AIを活用した高度な分析の実現や、AIエージェントを活用したセキュリティ運用の自律化を進めることで、顧客へのアラート通知/解決時間の短縮を目指します。当社はこの基盤を活用し幅広いお客様に訴求できる共通メニューをご用意することで、高品質・高性能でありながらコストパフォーマンスに優れたセキュリティサービスを提供し、お客様のセキュリティ対策強化に貢献していきます。

※1 MSSP: Managed Security Service Provider

※2 CFC/SOC: Cyber Fusion Center/ Security Operation Center



SIEM: Security Information and Event Management、セキュリティ情報及び各種機器のログを包括的に管理・分析するシステム
SOAR: Security Orchestration Automation and Response、セキュリティ運用の効率化を進めるためのツール

研究開発

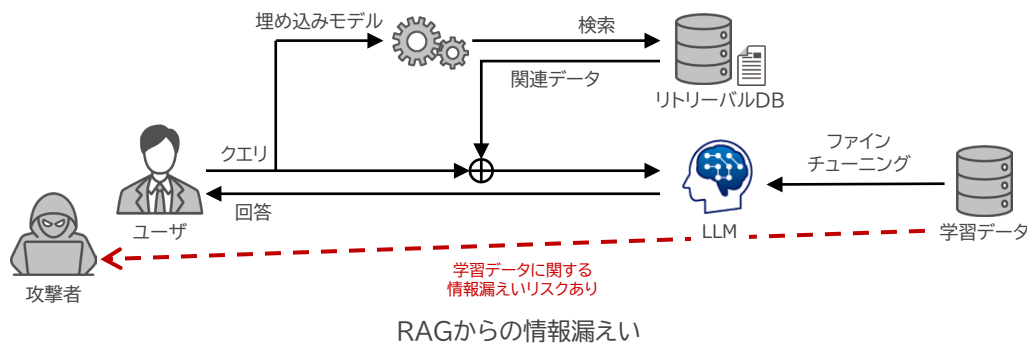
当社では、安定した社会活動を継続可能にするために、当社製品やサービスのセキュリティ向上に向けた研究開発に取り組んでいます。昨今、課題となっているAIを安全に使うための研究を紹介します。

AIの安全な活用を支える情報保護技術

近年、AI技術の普及に伴い、AIへの攻撃やプライバシー侵害などのリスクが社会的な課題となっています。国内外のAI関連ガイドライン・規格においても、「プライバシー保護」および「セキュリティ確保」の重要性が示されています。こうした背景を踏まえ当社は、安心・安全なAI搭載製品を顧客へ提供するため、「AIのセキュリティやプライバシーに関する研究開発」に取り組んでいます。

RAGにおける情報保護の課題

RAGは、大規模言語モデル(LLM)に外部情報を参照させて回答を生成する手法であり、モデルを再学習せずに知識を補えることから、LLMの学習データに由来する情報漏えいリスクを抑えられると期待されてきました。一方、当社の研究では、特定の攻撃条件下では、RAGを用いた場合でもLLMの学習データに関する情報漏えいリスクが残ることを発見しました。



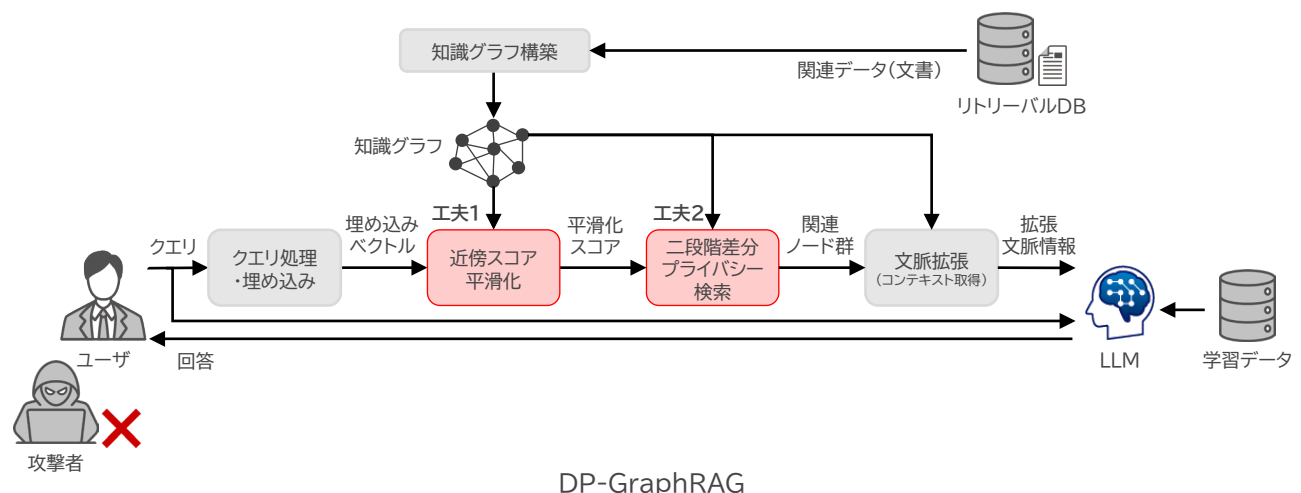
GraphRAGにおける情報保護と性能の両立

この課題を踏まえ、当社は、RAGの枠組みをベースに、文書に含まれる情報同士の関係を知識グラフとして活用するGraphRAGに、差分プライバシー(DP)の考え方を取り入れたDP-GraphRAGを提案しました。

DP-GraphRAGでは、検索時のスコアにノイズを加えて情報漏えいリスクの低減を図ります。

ただし、単純にノイズを加えるだけでは回答性能が低下するおそれがあるため、知識グラフ上の情報のつながりを活用し、回答に必要な情報を選びやすくする工夫を施しています。検証の結果、AIの回答の有用性を保ちながら、情報漏えいリスクを低減できる可能性を確認しました。

当社グループは、今後もAIと情報セキュリティの研究を進め、安心・安全なAI活用の実現に貢献していきます。



参考文献:

- Nakai, T., et al.: Does Retrieval-Augmented Generation Mitigate Training Data Leakage Risks from Large Language Models?, ESORICS2025 (ESORICS併設のAIセキュリティワークショップSECAIにてBest Paper Award受賞)
- 中井綱人、ほか: DP-GraphRAG: プライバシー実用性トレードオフを最適化する差分プライベートなGraphRAG, SCIS2026

第三者評価・認証

当社及び国内関係会社では、個人情報や情報セキュリティに関連する第三者評価・認証の取得を推進しています。

プライバシーマーク取得状況

プライバシーマーク取得状況(2026年4月1日現在)	
三菱電機株式会社	三菱電機デジタルイノベーション株式会社
株式会社アイプラネット	三菱電機ソフトウェア株式会社
エムビーテクノ株式会社	株式会社ダイヤモンドパーソネル
株式会社ビーシーシー	メルテック・ビジネス株式会社

ISMS認証取得状況

ISMS※1認証取得状況(2026年4月1日現在)	
三菱電機株式会社(神戸製作所 横浜事務所)	
三菱電機株式会社(電力システム製作所 電力ICTセンター)	
三菱電機株式会社(電子通信システム製作所)	
三菱電機株式会社(鎌倉製作所)	
三菱電機デジタルイノベーション株式会社 (芝浦オフィス、三田オフィス(株式会社テクノウェア含む)、中野オフィス(エムビーテクノ株式会社含む))	
三菱電機システムサービス株式会社(第3本部)	
三菱電機エンジニアリング株式会社(伊丹事業所)	
三菱電機エンジニアリング株式会社(鎌倉事業所)	
三菱電機ソフトウェア株式会社(電子システム事業統括部)	
三菱電機インフラテクニカ株式会社	
三菱プレジジョン株式会社	1. 営業本部における以下製品の防衛・宇宙分野向け営業 2. 鎌倉事業所における航空・宇宙・慣性・電波機器及びシミュレーションシステム 並びに駐車場システムの製造及び保守
三菱電機ディフェンス&スペーステクノロジーズ株式会社(東部事業部、北海道工場)	
三菱電機ディフェンス&スペーステクノロジーズ株式会社 (西部事業部(三田地区、三田ビル地区、伊丹地区、岩国地区、沖縄地区))	
株式会社ビーシーシー	

※1 ISMS:Information Security Management System

三菱電機株式会社
www.MitsubishiElectric.co.jp